UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/864,593	05/24/2001	Tommi Linnakangas	032986-016	2126

27045 7590 06/23/2006

ERICSSON INC.
6300 LEGACY DRIVE
M/S EVR C11
PLANO, TX 75024

EXAMINER	
TRUONG, THANHNGA B	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 06/23/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/864,593	LINNAKANGAS ET AL.	
	Examiner	Art Unit	
	Thanhnga B. Truong	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 April 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *8-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *8-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 May 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's amendment filed on April 11, 2006 has been entered. Claims 8-15 are pending. Claims 1-7 are canceled by the applicant and. Claims 8 and 11 are currently amended and claim 15 is newly added by the applicant.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 8-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ylonen et al (US 6,438,612 B1), and further in view of Nikander et al (US 6,253,321 B1).

a. *Referring to claim 8:*

i. Ylonen teaches:

(1) at least one Internet Protocol forwarder (IPFW) arranged to receive IP packets each of which is associated with a Security Association (SA), the at least one IP forwarder is further arranged to determine the destinations of the packets, and to forward the packets to their destinations **[i.e., referring to Figure 3, for Ylonen's invention to be applicable we will assume that some arbitrary protocol (where IP forwarder could include in this protocol) exists for setting up a context for securely tunneling data packets from the transmitting device 301 through the connection 303 to the receiving device 302. As an example we will consider the IKE and IPSEC protocols mentioned previously. Setting up said context will then correspond to having a negotiation between the two devices, during which negotiation they will first authenticate themselves to each other and thereafter agree upon a shared secret, an authentication and/or encryption method to be used for the communication and on a security parameter index (SPI) value. The results of the negotiation will be locally stored at both devices,**

which is illustrated in FIG. 3 with the schematic memory blocks 304 and 305 (column 5, lines 56-67 through column 6, lines 1-2). In addition, Using the language of the IKE and IPSEC protocols, the result of the negotiation between the devices 301 and 302 is a security association (or a well-defined group of security associations) (column 6, lines 58-61 of Ylonen)];

(2) a plurality of security procedure modules coupled to the IP forwarder(s) and arranged to implement security procedures for received IP packets in parallel **[i.e., referring to Figures 6 & 7, it is possible to have in each physical computer device 601 only a single module 602 performing IPSEC processing, and to have e.g. all virtual routers 603a, 603b and 603c in a physical router share the same IPSEC module. In an alternative architecture according to FIG. 7 each virtual router 703a, 703b and 703c can have its own IPSEC processor 702a, 702b and 702c, but the different processors have a shared data structure 704 that they use for allocating SPI values (either by actually having a single store for SAs or SPIs, or by checking the SPIs used by every other virtual router before allocating an SPI value). In a third alternative architecture the range of possible SPI values may be partitioned so that the virtual router identifier is encoded into the SPI value (either in a fixed number of bits, or using any suitable arithmetic coding method to combine a virtual network identifier and a SPI index). Variations and intermediate forms of these architectures can also be used. When there are multiple IPSEC processing modules, and the SPI can be used to identify the IPSEC processing module, no explicit virtual network identifiers are needed (column 8, lines 46-66 of Ylonen)]**; and

(3) a security controller (i.e., IPSEC engine) arranged to allocate negotiated SAs amongst the security procedure modules and to notify the security procedure modules and the IP forwarder(s) of the allocation, whereby the at least one IP forwarder can send IP packets to the security procedure module implementing the associated SA **[i.e., Figure 4 shows more detailed view of a transmitting device 401, a receiving device 402 and two-way communication connection 403 between them. Both the transmitting device 401 and the**

receiving device 402 have an automatic key manager block 404 and an IPSEC block 405 that communicate with a security policy database 406. We may keep the previously made assumption that the automatic key manager blocks 404 apply the IKE protocol for setting up the security association (column 7, lines 18-26 of Ylonen)].

ii. Although Ylonen is silent on the capability of a security controller (i.e., IPSEC engine) in Figures 3 and 4, the negotiation process that Ylonen has mentioned in these two Figures should at least include a controller included in the communication in order to establish an entire IP Security Association. However, Nikander teaches:

(1) Referring to Figure 3, the IPSEC engine must deal with security association creation and expiration and consult external key managers. In the invention, compiled filter code forms the core of the control logic of an IPSEC engine. The filter code controls the processing of incoming and outgoing packets, controls the application of transforms applied to data packets, and makes policy decisions about packets to be dropped or passed without applying transforms. The filter code communicates with a separate policy manager that makes the actual policy decisions and generates new compiled filter code according to need. The need for new compiled filter code potentially arises each time when the IPSEC engine receives a packet that it can not handle according to the existing compiled filter code. The policy manager then implements the policy for the packet causing the "trouble" and for similar future packets **(column 4, lines 38-53 of Nikander).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have included a IPSEC engines in Ylonen's invention concerning the secure transmission of data packets in a network.

iv. The ordinary skilled person would have been motivated to:

(1) have included a IPSEC engine in Ylonen's invention since it is an object of the invention that it is applicable in the course of secure tunneling

of data between virtual routers irrespective of the actual method of implementing the packet authentication and/or encryption **(column 3, lines 52-55 of Ylonen).**

b. *Referring to claims 9-11:*

i. These claims have limitations that is similar to those of claim 12, thus they are rejected with the same rationale applied against claim 12 below.

c. *Referring to claim 12:*

i. Ylonen further teaches:

(1) wherein the security controller is coupled to an Internet Key Exchange (IKE) module which is responsible for negotiating SAs with peer IKE modules, and the security controller is arranged to receive from the IKE module details of negotiated Sas **[i.e., Figure 4 is a slightly more detailed view of a transmitting device 401, a receiving device 402 and two-way communication connection 403 between them. Both the transmitting device 401 and the receiving device 402 have an automatic key manager block 404 and an IPSEC block 405 that communicate with a security policy database 406. We may keep the previously made assumption that the automatic key manager blocks 404 apply the IKE protocol for setting up the security association Furthermore, once the negotiation between the automatic key managers 404 is complete and the new security association is set up, both the transmitting device and the receiving device enter the information describing the security association into their security policy database. The stored information is then used for the processing of individual packets (column 7, lines 18-51 of Ylonen)].**

d. *Referring to claim 13:*

i. Nikander further teaches:

(1) wherein at least one of the at least one IP forwarder, security procedure modules, and security controller are implemented in software (i.e., process) or in hardware (i.e., device), or in a combination of hardware and software **[i.e., a device or process responsible for implementing the packet transformations according to the IPSEC method in a network device is generally called an "IPSEC packet processing engine" or an "IPSEC engine" for short.**

According to the invention, the operations to be performed on incoming and/or outgoing packets may in general be represented by means of a certain filter code, although the requirements for a filter code in an IPSEC policy application are much more complicated than in the simple packet filtering case referred to above in the description of prior art. A known packet filter simply sorts incoming packets into acceptable and non-acceptable packets. An IPSEC engine must deal with the security policy, the currently active security associations and the transforms between incoming and outgoing packets (column 4, lines 24-37 of Nikander].

e. *Referring to claim 14:*

i. This claim consist a method of processing IP packets at a network networking device to implement claim 1 and is rejected with the same rationale applied against claim 1 above.

f. *Referring to claim 15:*

i. Ylonen further teaches:

(1) wherein the security procedure modules are coupled together to allow the forwarding of an IP packet from one security procedure module to another **[i.e., Figure 4 is a slightly more detailed view of a transmitting device 401, a receiving device 402 and two-way communication connection 403 between them. Both the transmitting device 401 and the receiving device 402 have an automatic key manager block 404 and an IPSEC block 405 that communicate with a security policy database 406. We may keep the previously made assumption that the automatic key manager blocks 404 apply the IKE protocol for setting up the security association Furthermore, once the negotiation between the automatic key managers 404 is complete and the new security association is set up, both the transmitting device and the receiving device enter the information describing the security association into their security policy database. The stored information is then used for the processing of individual packets (column 7, lines 18-51 of Ylonen)].**

Response to Argument

4. Applicant's arguments filed on April 11, 2006 have been fully considered but they are not persuasive.

Applicant argues that:

Ylonen does not teach or disclose a security controller, as in the Applicant's invention, that allocates negotiated Security associations (Sas) among Security Procedure modules and notifies both the IPFWs and the security procedure modules.

Examiner disagrees with the applicant and still maintains that:

According to Ylonen's invention, data packets are communicated between a transmitting virtual router in a transmitting computer device and a receiving virtual router in a receiving computer device. A security association is established for the secure transmission of data packets between the transmitting computer device and the receiving computer device. The transmitting virtual router and the receiving virtual router are identified within said security association. In the transmitting computer device, **the security association for processing a data packet coming from the transmitting virtual router is selected on the basis of the identification of the transmitting virtual router within the security association (emphasis added).** In the receiving computer device, **the security association for processing a data packet coming from the transmitting computer device is selected on the basis of values contained within the data packet (emphasis added).** In the receiving computer device, the data packet processed within the security association is directed to the receiving virtual router on the basis of the identification of the receiving virtual router within the security association. Ylonen's invention is very much similar to applicant's invention for processing IPsec data packets. Therefore, by using only Ylonen, the rejection could have been proper and sufficient (see Ylonen's abstract). Although Ylonen is silent on the capability of a security controller (i.e., IPSEC engine) in Figures 3 and 4, the negotiation process that Ylonen has mentioned in these two Figures should at least include a controller included in the communication in order to establish an entire IP Security Association. However, Nikander teaches:

Referring to Figure 3, the IPSEC engine must deal with security association creation and expiration and consult external key managers. In the invention, compiled filter code forms the core of the control logic of an IPSEC engine. The filter code controls the processing of incoming and outgoing packets, controls the application of transforms applied to data packets, and makes policy decisions about packets to be dropped or passed without applying transforms. The filter code communicates with a separate policy manager that makes the actual policy decisions and generates new compiled filter code according to need. The need for new compiled filter code potentially arises each time when the IPSEC engine receives a packet that it can not handle according to the existing compiled filter code. The policy manager then implements the policy for the packet causing the "trouble" and for similar future packets **(column 4, lines 38-53 of Nikander).**

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the combination of teachings between Ylonen and Nikander are sufficient.

Applicant further argues that:

The applicant discloses Security Procedure modules as integral to the invention and the "...main modules in IPSec packet handling." (para [0061]). The portion of Ylonen cited as disclosing a plurality of security procedure modules actually discloses multiple IPSEC engines while the present invention discloses an IPSec engine comprising multiple Security Procedure modules.

Examiner again disagrees and still maintains that:

There are several possible architectures for implementing the present invention, in particular with respect to the selection of the SPI values. Some of these architectures are illustrated in Figures 6 and 7. **Firstly, according to Figure 6, it is**

possible to have in each physical computer device 601 only a single module 602 performing IPSEC processing, and to have e.g. all virtual routers 603a, 603b and 603c in a physical router share the same IPSEC module (emphasis added). In an alternative architecture according to Figure 7 each virtual router 703a, 703b and 703c can have its own IPSEC processor 702a, 702b and 702c, but the different processors have a shared data structure 704 that they use for allocating SPI values (either by actually having a single store for SAs or SPIs, or by checking the SPIs used by every other virtual router before allocating an SPI value). In a third alternative architecture the range of possible SPI values may be partitioned so that the virtual router identifier is encoded into the SPI value (either in a fixed number of bits, or using any suitable arithmetic coding method to combine a virtual network identifier and a SPI index). Variations and intermediate forms of these architectures can also be used. When there are multiple IPSEC processing modules, and the SPI can be used to identify the IPSEC processing module, no explicit virtual network identifiers are needed. Likewise, when a set of security associations is associated with each virtual router, the virtual router identifier does not need to be used explicitly as a selector, even though it is implicitly involved.

Furthemore, in response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., Security Procedure modules as integral to the invention and the "...main modules in IPSec packet handling" and IPSec engine) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

In addition, Ylonen also discloses one advantageous way of selecting a security association for the processing of a packet has been described in a co pending US patent application of the same applicant with the title "Method and Arrangement for Implementing IPSEC Policy Management using Filter Code". Other possible ways include the use of hash tables or lists of policy rules, which is incorporated by reference of Nikander. Nikander teaches a data processing system implements a security

protocol based on processing data in packets. The data processing system comprises processing packets for storing filter code and processing data packets according to stored filter code, and a policy managing function for generating filter code and communicating generated filter code for packet processing. The packet processing function is arranged to examine, whether the stored filter code is applicable for processing a certain packet. If the stored filter code is not applicable for the processing of a packet, the packet is communicated to the policy managing function, which generates filter code applicable for the processing of the packet and communicates the generated filter code for packet processing, which are met by claims 10 and 11.

Moreover, Ylonen further discloses in Figure 4, a slightly more detailed view of a transmitting device 401, a receiving device 402 and two-way communication connection 403 between them. Both the transmitting device 401 and the receiving device 402 have an automatic key manager block 404 and an IPSEC block 405 that communicate with a security policy database 406. We may keep the previously made assumption that the automatic key manager blocks 404 apply the IKE protocol for setting up the security association Furthermore, once the negotiation between the automatic key managers 404 is complete and the new security association is set up, both the transmitting device and the receiving device enter the information describing the security association into their security policy database. The stored information is then used for the processing of individual packets (column 7, lines 18-51 of Ylonen), which are met by claims 9 and 15.

Thus, Ylonen and Nikander do not need to disclose anything over and above the invention as claimed in order to render it unpatentable or anticipate. A recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claimed limitations.

For the above reasons, it is believed that the rejections should be sustained.

Conclusion

5. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The central fax number for the organization where this application or proceeding is assigned is 571-273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

TBT
June 19, 2006

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100